Testimony of

Dr. Hratch G. Semerjian
Acting Director

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

before the

Subcommittee on Disaster Prevention and Prediction
Committee on Commerce, Science & Transportation
United States Senate

"Scientific Research in Support of Homeland Security"

June 8, 2005

Introduction

Chairman DeMint and Members of the Committee, I am Hratch Semerjian, acting Director of the National Institute of Standards and Technology (NIST), part of the Technology Administration of the Department of Commerce. Thank you for this opportunity to testify about the contributions of NIST to homeland security. In accomplishing this and all parts of its mission, NIST works in many ways with companies, universities, and other government agencies to help protect our nation against terrorism.

Since World War II, our nation's greatest resources for homeland and national security have been a strong economy and a technological edge based on innovation. NIST has the unique mission of providing the measurements and standards infrastructure that the private sector, universities, and government agencies need to develop new technologies, products and services, conduct research, and effectively carry out their responsibilities. NIST measurements and standards and our support of new technologies have strengthened our economy and enabled the development and effective deployment of new homeland security technologies.

NIST's long and productive history of supporting homeland and national security efforts began shortly after its founding as the National Bureau of Standards. Partly in response to the Baltimore fire of 1904, Bureau researchers worked on the development of a national standard for hose couplings as well as a standard for an interchangeable device for nonstandard couplings. Other examples include crucial support for the development of nuclear weapons, aircraft instruments, and other technologies that helped the U.S. succeed in past conflicts. With its long experience as well as a diverse array of expertise, NIST was able to quickly respond to the terrorist attacks of 2001.

NIST currently has about 100 programs, supported by approximately $60 million in direct appropriations augmented by significant funding support from other agencies. This research is coordinated with the Department of Homeland Security (DHS) through a Memorandum of Understanding signed in 2003 between former Under Secretary for Technology, Phillip Bond, and Under Secretary for Science and Technology at DHS, Charles McQueary. In addition, other long standing relationships with the Department of Justice, the State Department, the National Security Agency, and the Office of Management and Budget also ensure that NIST's research is sufficiently coordinated. NIST's homeland security research spans the following areas:

- Chemical, biological, radiological, nuclear, explosive threat detection and remediation
- Safety of buildings and structures
- Safety and effectiveness of emergency responders
- Transportation system safety
- Information security
- Critical infrastructure protection
- Biometric identification
- DNA identification and diagnostics

This afternoon I would like to describe NIST's response to 9/11, and then share just a few examples of other NIST research supporting homeland security.

NIST response to 9/11 and the World Trade Center report

As I previously stated NIST responses to the terrorist attacks of 2001 were swift. Shortly after September 11, 2001, NIST building and fire experts joined teams of scientists and engineers in assessment of how the Pentagon as well as the World Trade Center buildings were severely damaged or collapsed in the attacks. Two months later, NIST experts presented to the U.S. Army Corps of Engineers a report of recommendations for rebuilding and retrofitting the Pentagon that would improve the Pentagon's resistance to similar attacks. NIST also provided assistance to the New York City medical examiner in identifying victims of the World Trade Center by validating existing methods and devising new DNA analysis techniques to allow identifications that would not otherwise have been possible due to small and degraded samples. In addition, NIST contributed expertise on life-cycle cost analysis and priority setting that are key components of the risk assessment guide issued by the Federal Emergency Management Agency (FEMA) to mitigate potential terrorist attacks against buildings.

After the October 2001 bioterrorist attacks, NIST worked with federal agencies and the private sector to ensure that commercial radiation facilities could effectively sterilize U.S. mail contaminated with anthrax. NIST worked with the Armed Forces Radiobiology Research Institute in Bethesda, the U.S. Postal Service, and other agencies to solve this challenging problem.

When the Hart Senate Office Building in Washington, D.C. was contaminated with anthrax, NIST experts in ventilation systems and indoor air quality modeled the different ways air flow in the building may have disseminated the anthrax spores. These models helped the Environmental Protection Agency plan the decontamination of the building. Since then, similar models have been used to evaluate protection technologies such as air filters, air cleaners, and sensor-driven ventilation systems, and one was incorporated into the Immune Building Toolkit developed by the Defense Advanced Research Projects Agency (DARPA).

The collapse of New York City's World Trade Center structures was among the worst building disasters in recorded history. As part of its larger effort to save lives in future terrorist attacks or natural disasters, NIST has been carrying out a response plan with three parts:

- A building and fire safety investigation of the probable causes of the WTC tower collapse after terrorists flew jet-fuel laden airliners into the buildings, and the associated evacuation and emergency response procedures.
- A research and development program to provide the technical basis for improved building and fire codes, standards, and practices.
- A dissemination and technical assistance program to engage leaders of the construction and building community in implementing proposed changes to practices, standards and codes.

The investigation was conducted with $16 million in funding by the U.S. Congress from an emergency supplemental appropriation and transferred to NIST from FEMA. It builds on the findings and recommendations of an earlier WTC building performance study conducted jointly by FEMA and the American Society of Civil Engineers.

The investigation's analysis, which is the most detailed examination of a building failure ever conducted, established the probable sequences for the collapse of each tower:

1. The aircraft impact severed perimeter columns, damaged interior core columns, and dislodged fireproofing off structural beams.
2. The fires, which were initiated by jet fuel but fed by building contents such as furniture and paper, weakened the building core.
3. The fires also weakened floors, which sagged and pulled inward on the perimeter columns.
4. The fire weakened perimeter columns bowed inward and buckled due to the floor pull-in forces, leading to collapse.

Along with this analysis, NIST released in April drafts of 15 reports from three projects of the investigation:

- analysis of building and fire codes and practices
- occupant behavior, egress and emergency communications
- fire service technologies and guidelines

Recommendations for improvements to building and fire codes, standards and practices derived from these and the other five projects in the investigation will be released for public comment later this month, along with the draft of the final investigation report and drafts of 27 reports from the remaining five projects.

Additional Homeland Security Research

NIST, with its diverse research portfolio is also supporting the nation's homeland security efforts in a number of ways that are not directly related to the attacks of 9/11.

Cybersecurity

Cybersecurity work at NIST plays a key role in addressing the urgent need to improve the cybersecurity posture of the Nation, and in particular that of the Federal government. Some examples of recent and continuing NIST work in this field are:

- NIST is developing minimum security controls for <u>all</u> federal computer systems. This effort will have a huge impact on the nation. These minimum security controls will be mandatory for federal agencies, although we expect they may become a *de facto* standard in the private sector as well.
- NIST continues to publish a wide range of cybersecurity standards and guidelines, which are available free on NIST's Web site. These are frequently used by the private sector, state and local governments, and even some foreign governments. Our contingency planning guideline alone was downloaded more than 400,000 times during the first year it was available.
- Homeland Security Presidential Directive #12, which mandates a common identification standard for all federal employees and contractors, requires NIST to develop a series of standards leading to reliable and secure "smart cards". NIST computer security specialists worked closely with other federal agencies—including the Office of Management and Budget, the Office of Science and Technology Policy, and the Departments of Defense, State, Justice, and Homeland Security—as well as private industry, to develop Federal

Information Processing Standard 201, Personal Identity Verification of Federal Employees and Contractors.

- NIST is supporting the Small Business Administration in security outreach activities to small businesses.
- NIST is developing cryptographic standards for "constrained environments". An example is a "smart card" with limited memory and little or no computing power.
- NIST is beginning work to develop security checklists for computer systems that control buildings and manufacturing processes.
- NIST is developing the National Vulnerability Database, a comprehensive information technology database and search engine that integrates all publicly available US Government vulnerability resources and provides links to industry resources.
- NIST is working to develop metrics for the effectiveness of software assurance tools, and assessing current methods and tools in order to identify deficiencies which can lead to software product failures and vulnerabilities.
- NIST continues to develop security guidelines/best practices on risk assessment, media destruction and sanitization, desktop IT security scenarios, and malware mitigation measures.

Additionally, NIST's Hollings Manufacturing Extension Partnership is beginning its outreach activities to small and medium sized manufacturers by providing them guidance with vulnerability assessments, business continuity, and supply chain implications.

Biometrics

As part of its fulfillment of the Patriot Act, NIST conducted the Fingerprint Vendor Technology Evaluation in 2003. The eighteen competing companies used 34 different fingerprint matching systems. The evaluation, which was based on fingerprint data from a variety of U.S. and state government sources, tested performance accuracy for various numbers and types of fingerprints.

The evaluation demonstrated the significance of fingerprint quality as well as the number of fingers used. (The matching accuracy using four fingers was better than the accuracy using only two fingers, which in turn was better than single-finger matching.) The test also showed that the most accurate fingerprint systems perform better than the most accurate facial recognition systems, even when using only a single fingerprint.

NIST's key Patriot Act recommendations included in the report to Congress titled "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents" dated February 2003:
:

1. For verification ("one-to-one matching" to establish that the person is who he/she claims to be), NIST recommends one face image and two index fingerprints.
2. For identification ("one-to-many matching" to find the identity of a person in a large database), NIST recommends ten slap fingerprint images for enrollment and checking of large databases. Face images are not recommended.

The Consolidated Appropriations Act, 2005, provided an increase of $2.0 million to NIST's biometric program. This new funding will allow NIST to begin testing the accuracy of

multimodal systems, develop guidelines for testing fingerprint segmentation methods, and determining the influence of multiple images on the accuracy of facial biometrics.

Radiation detectors

NIST, in cooperation with the American National Standards Institute (ANSI), has an extensive program to develop and support standards for the radiation detectors used by first responders and for other homeland security applications. The standards will help first responders and government agencies make better use of existing equipment and acquire the right equipment for emergency response, and they will encourage manufacturers to better design instruments and represent their specifications to agency and responder buyers.

This program includes:

- Leadership in the development of the four ANSI standards that are currently released. These standards cover electronic personal alarming detectors (called “pagers”), personal radiation dosimeters, portable instruments, radionuclide identifiers (specialized devices that can identify specific radioactive materials), and portal monitors.
- Ongoing development of newer standards, such as for portal monitors with radionuclide identification.
- Leadership in the development of test and evaluation protocols for determining whether such radiation detectors meet the technical requirements of the new ANSI standards.

As an example of the application of the new standards, NIST recently tested 31 commercial detectors, including hand-held survey meters, pagers, and radionuclide identifiers. Federal, state, and local agencies are using such instruments as part of homeland security-related efforts to detect and identify radioactive materials. The tests determined that portable radiation detectors generally perform well against the new consensus standards but provided inaccurate readings for certain types of radiation. Researchers compared the device readings to NIST measurements for different radiations levels. The majority of the detectors agreed with NIST-measured values but some detectors tested had large discrepancy in readings for the lowest-energy X-rays, and were much larger than those stated in manufacturers' specifications.

Other examples of NIST work related on radiation detectors include the following:

- Technical guidance for emergency responders.
- Development of a test bed for evaluating hand-held radiological detectors and truck portal monitors.
- Development of NIST-traceable test sources for gamma rays and neutrons used in calibrations of detectors.
- Development of methods, testing materials, standard reference materials, and measurement validations for radiological clean-up and mitigation.

Public Safety Communications Interoperability

NIST's Office of Law Enforcement Standards (OLES) is the common technical thread that is working to facilitate local, state, and Federal communications interoperability efforts through the

consensus standards process. Funded through SAFECOM, a program of DHS's Science and Technology Directorate's Office for Interoperability and Compatability, the Department of Justice's Community Oriented Policing Service, and the Advanced Generation of Interoperability for Law Enforcement (AGILE) program, OLES has been employing a structured approach for confronting interoperability standardization issues. This standardization strategy is centered on the development of an architectural framework that satisfies the real-world requirements of public safety responders. The framework defines the overall structured approach for facilitating interoperability. Functional Standards (in the form of Interface Specifications) then define the details of the structure, and indicate how the architecture (and its components) will operate. Although progress has been slow in the development of these standards, significant progress has been achieved within the last year. OLES helped to complete the Public Safety Statement of Requirements for Wireless Communications and Interoperability on behalf of SAFECOM in March 2004. This is the first comprehensive, practitioner-accepted, record of the telecommunication needs of the public safety community within and across local, state, Federal, and tribal boundaries.

Additionally, OLES on behalf of DHS SAFECOM, produced a draft of an architectural framework which is in essence a map that shows a network of networks and a system of systems approach which will be employed by public safety in the future. In response to Congress' call for immediate standards for communications interoperability, NIST, along with DHS and DOJ, have developed a partnership with public safety leadership to either significantly accelerate the current P25 standards development or develop interim communications standards in the absence of P25 standards. Additionally, Congress requested that SAFECOM produce a report on the plan for accelerating the development of national voluntary consensus standards for public safety interoperable communications. It is expected that because of the recent efforts by NIST and its partners, key interoperability standards will be published by the end of 2005, and products employing these standards would be available by the end of 2006.

Operations in collapsed buildings

In 2001, search-and-rescue robots that had been tested on a special NIST course penetrated areas too small and too hazardous for emergency responders to locate remains of several victims at the World Trade Center site. At that time, NIST already had expertise with collapsed buildings, including setting up competitions designed to accelerate the development and testing of urban search-and-rescue robots. Last year, NIST organized competitions in New Orleans, San Jose, and Lisbon, Portugal. More broadly, NIST has launched a DHS-funded multi-year program to develop comprehensive standards and performance metrics for urban search-and-rescue robots.

Collapsed buildings also present a significant problem in terms of radio communications. First responders who rely on radio communications often lose signals in shielded or complex environments such as in steel and reinforced concrete high-rise structures, and in the basements or elevator shafts of buildings. It also is very difficult to detect radio signals through the dense rubble of a building that has collapsed as a result of natural disasters or terrorist attacks. To simulate disaster environments, NIST is using real-world "laboratories"—buildings that are scheduled to be imploded as part of construction and recycling projects — such as the old Washington Convention Center and Veterans Stadium in Philadelphia. After the implosion,

NIST researchers studied various schemes for detecting signals by searching with directional antennas and by connecting detectors to metal debris found within the rubble of the building. A technical report on these experiments will be published this summer.

Forensic analysis of magnetic audio tapes

NIST recently developed a real-time magnetic imaging system that enables crime investigators to "see" signs of tampering in audio tapes, such as erasing and overdubbing. The new system, which permits faster screening and more accurate audiotape analysis than previously possible, was recently delivered to the Federal Bureau of Investigation (FBI) Forensic Audio Analysis, which receives hundreds of audiotapes annually for analysis. Representing evidence from crimes such as terrorism, homicide and fraud, these tapes come from a wide variety of devices, including answering machines, cassette recorders and digital audiotape recorders. The benefits of the NIST system are its speed in correlating sounds with magnetic marks on tape, and the fact that it makes an image without damaging the tape.

Detection of explosives and toxic chemicals

The cost and size of devices for detecting toxic airborne chemicals largely limits them to specialized equipment designed for use by the military or by first responders to chemical spills. In the event of an attack involving toxic chemical agents—such as the sarin gas attack in a Tokyo subway station—such portable detectors typically would not arrive on the scene until after victims had been harmed.

NIST is conducting research on a class of microsensors that has the potential to serve as a cost-effective early warning system for toxic gases and may also be applicable to the detection of vapors from explosive materials. The NIST devices use an array of microscopic hotplates coated with a film that is sensitive to ambient chemicals. A key advantage of this technology is that various types of films can be combined with multiple types of temperature cycles. An array of hotplates can thus produce a "signature" that can be matched against a library of chemical signatures to identify both the type and concentration of the toxic gas. Another advantage is that the microsensors can be produced inexpensively with electronic processing circuits built in. Preliminary testing at the Army's Edgewood Arsenal has confirmed that 1-part-per-million sensitivity is feasible with actual chemical warfare agents.

Standards Development Organizations

Besides the research done in our laboratories, NIST works with private sector Standards Development Organizations (SDO's) on the implementation of homeland security standards.

- NIST assisted the DHS Science and Technology Directorate, Standards Portfolio in developing and implementing a formal procedure for the adoption of standards.
- NIST is assisting DHS in the coordination of public and private resources for the development of technical standards that support homeland security. The primary focus of this coordination is the American National Standards Institute's Homeland Security Standards Panel, which is co-chaired by Mary Saunders of the NIST Standards Services Division.

- NIST recently leveraged its technical expertise in ion mobility spectrometry (IMS) to establish minimum performance requirements and an associated test method for detectors of trace explosives based on IMS. Although some first responders already use IMS trace detection equipment, a documentary standard was needed to address the wide variety of possible future uses. The standard was developed with input from six detector manufacturers, state and local government agencies, federal agencies such as U.S. Coast Guard, the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Transportation Security Administration, and security professionals such as the U.S. Secret Service.

Conclusion

As the Committee can see by the few examples I have cited, NIST has a very diverse portfolio of research activities supporting our nation's homeland security effort. After the terrorist attacks of 9/11, NIST responded to the research challenges it faced. NIST's long history of research supporting homeland and national security is helping to enable the development and effective deployment of new technologies to protect the homeland. Once again thank you for inviting me to testify about NIST's activities and I would be happy to answer any questions you may have.